EGNYTE

# Data Privacy in Clinical Trials

## A Best Practices Guide

# Introduction

As life sciences companies grow, the regulatory compliance requirements, and risks, expands as well. These responsibilities extend beyond conventional health-related frameworks (e.g. GxP, HIPAA, etc.) but into the realm of data privacy as well.

For high-growth institutions with limited resources & bandwidth, the question arises: what should you do?

In this document, we chronicle some of the regulations affecting the life sciences industry and share 5 activities to help your organization comply with these new and dynamic laws. Though not comprehensive, we hope they provide you with a right-sized approach for your organization.

# Data Privacy Regulations Impacting Life Sciences

### Trial-related frameworks and concepts

International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use (ICH), Good Clinical Practice (GCP), Protected Health Information (PHI), Personally Identifiable Information (PII), Standard Operating Procedure (SOP)

### Regional data privacy regulations

IUS Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), California Consumer Privacy Act (CCPA), EU's General Data Protection Regulation (GDPR) and Clinical Trials Regulation (CTR), China's National Medical Products Administration (NMPA-GCP-No57-2020), Japan's Act on Personal Information Protection, and Australia's National Statement on Ethical Conduct in Human Research (G-NatlStmt)

# Five Best Practices to Implement

## **#1 -** Audit your processes for more than just Quality

Many companies perform internal & supplier audits to manage the compliance envelope for a company. However, in the world of data privacy laws, you have to extend your audit practices to encompass more than SOPs and records, for example.

**Things to consider**

- What data types will you be receiving? Do they contain sensitive information?
- If you're working with external vendors (e.g. sites, CROs, data providers, etc.), then you will need to ask the same questions of them.
- What software will touch this data? Email? Content repositories? Cloud analytics?
- What are the sources of regulated data?
- Who is interacting with sensitive data?

## **#2 -** Develop SOPs

SOPs are common for guiding how individuals should handle regulated (e.g. GMP, GCP, etc.) data. We recommend developing a similar set for complying with data privacy laws alongside. A collaboration between the business, IT, Quality, and Data Protection Officer (DPO), is paramount to develop a practical Standard Operating Procedures (SOP) for mitigating risk.

**Things to consider**

- Collaborate between key functional areas (IT, business, Quality, DPO, etc.)
- Make it mandatory for those engaged in regulated activities
- Codify remediation processes and escalation paths
- Who is interacting with sensitive data?
- Ensure simplicity of training & execution

## **#3 -** Centralize your data to minimize risk

In many companies with high-velocity programs, risks and gaps in compliance emerge when a myriad of systems are used and sensitive data resides in a multitude of locations. As a best practice, institutions are now centralizing their data into a single, controlled organizational repository to streamline processes, decrease costs, and mitigate risks.

**Things to consider**

- Identify a single, easy to use software platform for documents & data
- Ensure that the repository is GxP compliant
- Implementation should be fast
- The software should foster collaboration with relevant parties
- Integrates native ransomware protection
- Who is interacting with sensitive data?

## **#4 -** Train your staff

People are a critical part of ensuring you comply with data privacy laws. Training is the lynchpin. Train your team on an ongoing basis such that they have familiarity with the data types, SOPs, and corresponding exception handling.

**Things to consider**

- Frequency of training
- Have personnel to answer questions
- Use software to automate, digitize the training
- Leverage external resources (e.g. consultants) to bring in expertise

## **#5 -** Automate governance

Recent technological advances are able to automatically track & notify you of risks to data privacy. Innovations like machine learning and artificial intelligence (ML/AI) can seamlessly analyze the contents of your documents, rank them based on risk, and notify you when data or documents under the purview of these laws is present.

**Things to consider**

- Ensure these tools integrate directly with your repository (see Practice #3)
- Utilize alerts to notify administrators and log data privacy events
- Your tool should have classification & models built-in
- Who is interacting with sensitive data?
- Automation should leverage ML/AI

Science is becoming more distributed, global, and dynamic than ever before. Trial diversity and geographic diversification in clinical trials not only provide better outcomes but speed up certification in foriegn markets. But as dispersed trials spread across the jurisdictions, data privacy laws are a larger concern to product development, testing, and data management. With these 5 recommendations, you and your organization can mitigate risk and avoid non-compliance.

Book a Meeting



**Contact Us**

+44 20 3356 3714
5th Floor, The Pinnacle,
20 Tudor Road, Reading, RG1 1NH

www.egnyte.com